UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

CARNEL FAULKNER, individually and on behalf of all others similarly situated, Plaintiff, vs. MONEYGRAM PAYMENT SYSTEMS, INC., a corporation, Defendant.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Carnel Faulker individually and on behalf of all others similarly situated, ("**Plaintiff**") brings this Action against Defendant MoneyGram Payment Systems, Inc. ("**MoneyGram**" or "**Defendant**"). Plaintiff's allegations are based upon personal knowledge as to himself and his own acts, and upon information and belief as to all other matters based on the investigation conducted by and through Plaintiff's attorneys. Plaintiff believes that substantial additional evidentiary support will exist for the allegations set forth below, after a reasonable opportunity for discovery.

INTRODUCTION

1. MoneyGram is a leading global money transfer and payment services company, offering services in more than 200 countries and territories, operating "one of the largest cash distribution services in the world."[1] As of 2024, MoneyGram serves over 150 million customers and provides its MoneyGram platform to purportedly "enable seamless and secure transfers around the world."[2] Plaintiff and millions of other consumers entrusted MoneyGram with their personal data when they registered for accounts or each time they transferred money through the

[1] *About MoneyGram*, MoneyGram, available at https://corporate.moneygram.com/about-us/#Leadership (Last visited Oct. 9, 2024).
[2] *BamSEC* (February 23, 2024) available at, https://www.bamsec.com/filing/127393123000039?cik=1273931 (Last visited October 10, 2024).

MoneyGram platform (hereinafter, "**Platform**"), providing their names, contact information, social security numbers, government-issued identification numbers, bank account numbers, and prior transaction details and history.[3] As stated in its own privacy policy, MoneyGram recognizes the heavy burden of protection and security that it bears when collecting and storing this data.[4] MoneyGram further represents that it "use[s] a variety of robust physical, technical, organizational, and administrative safeguards to protect [customers'] personal data from unauthorized access, loss or alteration."[5] MoneyGram touts its purported dedication to strong security by making the following advertising claims for its devices and services, including but not limited to, the following:

- "We Lead the Industry in Protecting Customers."[6]
- "MoneyGram works diligently to prevent its systems from being used to perpetrate any unlawful activity."[7]
- "We are committed to safeguarding the privacy of your Personal Information."[8]
- "We use the appropriate organization, technical and administrative measures to maintain the security of your Personal Information and to protect against the destruction, loss, alternation, unauthorized disclosure, or access to Personal Information under our control."[9]

[3] *Consumer Data Notice* (2024, Oct. 7), MoneyGram, available at https://www.moneygram.com/intl/us-notice.
[4] *Global Privacy Notice*. (2023). MoneyGram, available at https://www.moneygram.com/intl/privacy-center/global-privacy-notice (Last visited Oct. 9, 2024).
[5] *Id.*
[6] *Compliance*, MoneyGram, available at https://corporate.moneygram.com/compliance/?_ga=2.240501386.802156005.1728503421-438024125.1728503421 (Last visited Oct. 8, 2024).
[7] *Id.*
[8] *Global Privacy Notice* (Apr. 1, 2022), MoneyGram, available at https://www.tbcbank.ge/web/documents/10184/666084/Updated-MoneyGram-Global-Consumer-Notice-Privacy-ENG.pdf/2ac2cb71-9efc-4ca0-a988-366fdcafddd2 (Last visited Oct. 8, 2024).
[9] *Id.*

- "We also take preventive measures to restrict access to Personal Information to only those who have need to know . . . All who have access to, or are associated with, the processing of Personal Information are contractually obligated to respect the confidentiality of your Personal Information."[10]

2. MoneyGram's representations of strong and transparent security have proved false and misleading—MoneyGram failed to safeguard the sensitive personal identifying information of millions of its consumers and failed to implement robust security measures to prevent this information from being stolen.

PARTIES

3. Plaintiff Carnel Faulker is a California resident who had his personal identifiable information and personal financial information ("personal identifiable information" and "personal financial information" are collectively "**Private Information**" **or "PII"**) exfiltrated and compromised in the data breach announced by Defendant on October 7, 2024. Plaintiff has regularly used MoneyGram for years, first using it to pay rent 8-10 years ago. To transfer money through the Platform, Plaintiff was required to provide two forms of identification, which included his government-issued driver's license number, and to fill out a form which listed his bank account information and his social security number. Plaintiff last transferred funds through the Platform during or around autumn of 2023. In total, Plaintiff was required to provide Defendant with his name, contact information, social security number, government-issued identification number, and bank account numbers, among other information. In making his decision to utilize the Platform to transfer money, Plaintiff reasonably expected that Defendant would safeguard his Private Information and destroy it after completing Plaintiff's request to send/receive money. Plaintiff would not have used the Platform for money transfers, if he knew that the sensitive information collected by Defendant would be at risk. Plaintiff has suffered damages and remains at significant risk now that his Private Information has been leaked online and/or otherwise compromised. As a result of this data breach, Plaintiff has spent substantial time in attempt to mitigate damages caused

[10] *Id.*

by this data breach, including monitoring all of his accounts and financial activity. The time spent dealing with Defendant's data breach is time Plaintiff otherwise would have spent it on other activities such as work and/or recreation. Plaintiff anticipates taking additional time-consuming and necessary steps to help mitigate the harm caused by the data breach, including continuously reviewing his accounts for any unauthorized activity.

4. Defendant MoneyGram Payment Systems, Inc. is a global money and transfer payment company. Defendant is a wholly-owned subsidiary of the publicly traded stock corporation MoneyGram International; Inc. Defendant's parent company is incorporated in Delaware and Defendant is headquartered in the city of Dallas, Texas.

JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. Section 1332 of the Class Action Fairness Act of 2005 because: (i) there are 100 or more class members, (ii) there is an aggregate amount in controversy exceeding $5,000,000, exclusive of interest and costs, and (iii) there is minimal diversity because at least one Plaintiff (CA) and Defendant (TX) are citizens of different states. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. Section 1367.

6. Pursuant to 28 U.S.C. Section 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District: Defendant is registered in Texas and headquartered in this District, Defendant gains revenue and profits from doing business in this District, consumers sign up for MoneyGram accounts, transfer money through the Platform and provide MoneyGram with their Prviate Information in this District, Class members affected by the breach reside in this District, Defendant has a corporate office in this District, and Defendant employs numerous people in this District.

7. Defendant is subject to personal jurisdiction in Texas as a resident of this state. Defendant is authorized to do and is doing business, advertises, and solicits business within the state. By residing in Texas, Defendant is physically present and subject to its laws.

FACTUAL ALLEGATIONS

8. MoneyGram is a leading global money transfer and payment services company. Founded in 1940, MoneyGram has grown to be one of the largest money transfer providers worldwide.[11] MoneyGram offers a wide range of financial services, including domestic and international money transfers, bill payments and mobile wallet transactions. MoneyGram serves over 150 million customers in more than 200 countries and territories, with a network of approximately 347,000 agent locations globally. The company utilizes various brands under its corporate umbrella, including MoneyGram, WalMart2World, and MoneyGram Online.[12]

9. MoneyGram collects and processes the personal data of millions of consumers, including sensitive personal and financial information. The information collected and stored by MoneyGram includes, but is not limited to, "***names, contact information (such as phone numbers, email and postal addresses), dates of birth… Social Security numbers, copies of government-issued identification documents (such as driver's licenses), other identification documents (such as utility bills), bank account numbers, MoneyGram Plus Rewards numbers, transaction information (such as dates and amounts of transactions)***."[13] MoneyGram collected this Private Information by requiring users to complete account registration and verify their identities to send funds through Platform and continues to collect and store this Private Information when users transfer money.

10. MoneyGram holds itself as a trustworthy company, which recognized and values the customers' privacy and personal information and has repeatedly assured its customers that it is "committed" to data security.[14]

11. MoneyGram's privacy policy and online advertisements clearly and unequivocally state that any personal information provided to MoneyGram will remain secure and protected,

[11] *Supra*, Note 1.
[12] *Id.*
[13] *Supra*, Note 3.
[14] *Supra*, Note 8.

driving the point home that *Defendant wants customers to believe their personal information will be safeguarded*:

> **At MoneyGram ("we," "us" and "our" will refer to the specific company with which you interact, and "MoneyGram" will refer to the MoneyGram group of companies), we respect your privacy and are committed to handling your personal data responsibly and in accordance with applicable laws.**[15]

12. Plaintiff and other similarly situated consumers relied to their detriment on MoneyGram's uniform representations and omissions regarding data security, including MoneyGram's failure to alert customers that its security protections were inadequate, and that MoneyGram would forever store Plaintiff's and customers' Private Information, failing to archive it, protect it, or at the very minimum warn consumers of the anticipated and foreseeable data breach.

13. Had MoneyGram disclosed to Plaintiff and its other customers that its data systems were not secure and were vulnerable to attack, Plaintiff would not have utilized MoneyGram's services.

14. Plaintiff and other similarly situated consumers trusted MoneyGram with their sensitive and valuable Private Information. MoneyGram did not need to store this Private Information at all. Once identities are verified, as Plaintiff was required to do *each time he transferred funds*, MoneyGram could delete government identification numbers. Instead, MoneyGram retains information to increase its profits, to gather information regarding its customers, and to track its customers and their behaviors.

15. MoneyGram knew or should have known that Plaintiff and Class Members would reasonably rely upon and trust its promises regarding security and safety of its data and systems.

16. By collecting, using, selling, monitoring, and trafficking Plaintiff's and other customers' Private Information, and utterly failing to protect it by maintaining inadequate security

[15] *Supra*, Note 4.

systems, failing to properly archive the Private Information, allowing access of third parties, and failing to implement security measures, MoneyGram caused harm to Plaintiff and consumers.

THE DATA BREACH

17. At all material times, MoneyGram failed to maintain proper security measures despite its promises of safety and security to consumers.

18. On September 27, 2024, MoneyGram detected unauthorized access to its systems between September 20-22.[16] [17] MoneyGram revealed that attackers had gained access through a social engineering attack on MoneyGram's IT help desk.[18]

19. MoneyGram publicly disclosed the data breach on October 7, 2024, approximately ten days after detecting unauthorized access.[19] It confirmed that sensitive customer information had been compromised, including names, contact details, dates of birth, Social Security numbers, copies of government-issued IDs, and bank account information.[20]

20. In its statement, MoneyGram does not disclose how many customers' Private Information was breached, leaving consumers to speculate whether it is likely that their Private Information has been compromised and without clear instruction on what they can do to protect themselves now that their PII has been exposed.

21. No adequate remedy at law. Plaintiff and the Class are entitled to equitable relief as no adequate remedy at law exists.

---

[16] Grieg, Jonathan (Oct. 8, 2024), *MoneyGram Says Customer Information Stolen During September Attack,* THERECORD, available at https://therecord.media/moneygram-says-customer-information-stolen (Last visited Oct. 9, 2024).
[17] Ardrey, Taylor (Oct. 9, 2024), *MoneyGram Announces Hack: Customer Data Such as Social Security Numbers, Bank Accounts Impacted,* AOL.com [via USA TODAY], available at https://www.aol.com/moneygram-announces-hack-customer-data-131627863.html (Last visited Oct. 9, 2024).
[18] Uliss, Ryan, *MoneyGram Confirms its Recent Cyberattack Exposed Sensitive Customer Data*, NATIONALCIOREVIEW, available at https://nationalcioreview.com/articles-insights/extra-bytes/moneygram-confirms-its-recent-cyberattack-exposed-sensitive-customer-data/ (Last visited Oct. 9, 2024).
[19] Binder, Matt, *MoneyGram Confirms Hack: Social Security Numbers, Driver's Licenses, and Other Customer Data Have Leaked,* MASHABLE, available at https://mashable.com/article/moneygram-data-breach (Last visited Oct. 8, 2024).
[20] *Supra*, Note 3.

i. MoneyGram has not yet implemented adequate protections to prevent a future data breach, nor has it given an adequate notice to all affected class members, and therefore, the equitable relief requested here would prevent ongoing and future harm;

ii. Injunctive relief is also necessary to prevent the members of general public from being misled by Defendant's misrepresentations regarding privacy and security of information;

iii. The equitable relief under the UCL also creates a straightforward cause of action for violations of law (such as statutory or regulatory requirements related to representations and omissions made with respect to Defendant's services). Furthermore, damages for non-UCL claims require additional elements or pre-suit notice letters, which would potentially eliminate possibility of providing damages to the entire class, while restitution would provide certainty and remedy for all affected victims.

iv. In addition, discovery—which has not yet been provided and/or completed—may reveal that the claims providing legal remedies are inadequate. At this time, forcing an election of remedies at the initial pleadings stage, in the absence of completed discovery regarding class certification and merits, is premature and likely to lead to subsequent, potentially belated, and hotly contested motions to amend the pleadings to add equitable remedies based on a lengthy historical recount of discovery and analysis of voluminous exhibits, transcripts, discovery responses, document productions, etc., as well as related motions to seal confidential information contained therein.

IMPACT OF DATA BREACH ON CONSUMERS

22. Plaintiff and the Class have suffered actual harm as a result of MoneyGram's conduct. MoneyGram failed to institute adequate security measures and neglected system vulnerabilities that led to a data breach. This breach allowed a hacker to access the Private

Information, including names, contact information dates of birth, Social Security numbers, government-issued identification documents, bank account numbers, and transaction information, for Plaintiff and the Class. This Private Information was accessed by a person who engaged in social engineering with the purpose of acquiring this information. Upon information and belief, the social engineer who accessed MoneyGram's systems is a criminal, and intends to either sell, trade, or otherwise operationalize to perpetuate scams, identity theft, and further social engineering schemes. Now that the Private Information is in the hands of a nefarious individual, it will continue to be at risk for the indefinite future. In fact, the U.S. Government Accountability Office found that, "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[21]

Digital Phishing Scams

23. Phishing scammers use emails and text messages to trick people into giving them their personal information, including but not limited to passwords, account numbers, and social security numbers. Phishing scams are frequently successful, and the FBI reported that people lost approximately $57 million to such scams in 2019 alone.[22]

24. Since the data breach, Plaintiff has experienced an increase in text messages from unknown numbers with embedded links. Given the perpetrator's willingness to engage in social engineering scams, it comes as no surprise that Plaintiff's and Class Members' information is now being used to conduct further scams.

25. MoneyGram's customers are now more likely to become victims of digital phishing scams because of the released personal information.

SIM-Swap

26. The data leak can also lead to SIM-swap attacks against the Class.[9] A SIM-swap attack occurs when the scammers trick a telephone carrier to porting the victim's phone number to

[21] *See* U.S. GOV'T ACCOUNTABILITY OFF. REPORT TO CONGRESSIONAL REQUESTERS 2007, available at https://www.gao.gov/new.items/d07737.pdf (Last visited April 1, 2024).
[22] *See How to Recognize and Avoid Phishing Scams*, FTC Consumer Advice, available at https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (Last visited April 1, 2024).

the scammer's SIM card. By doing so, the attacker is able to bypass two-factor authentication accounts, as are used to access cryptocurrency wallets and other important accounts. The type of personal information that has been leaked poses a profound tangible risk of SIM-swap attacks for the Class.

27. MoneyGram's customers are now more likely to become victims of SIM Swap attacks because of the released personal information.

Loss of Time

28. As a result of this breach, Plaintiff and impacted consumers will suffer unauthorized email solicitations, and experience a significant increase in suspicious phishing scam activity via email, phone calls, text messages, all following the breach.

29. Plaintiff, in great distress, is attempting to change his passwords and associated accounts which may be connected to various pieces of stolen Private Information. Plaintiff has been monitoring his credit activity, now living in fear and apprehension of further attacks.

Overpayment for Platform Fees

30. Plaintiff and the Class would not have utilized the Platform if they knew that doing so would result in their Private Information being compromised and exfiltrated. Thus, they overpaid the associated fees on their money transfer transactions based on how the Platform was represented compared to what they received.

Threat of Identity Theft

31. As a direct and proximate result of MoneyGram's breach of confidence, and failure to protect the Private Information, Plaintiff and the Class have also been injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, and other misuse of this Private Information, resulting in ongoing monetary loss and economic harm, loss of value of privacy and confidentiality of the stolen Private Information, illegal sales of the compromised Private Information on the black market, mitigation expenses and time spent on credit monitoring, identity theft insurance, credit freezes/unfreezes, expenses and time spent in initiating fraud alerts, contacting third parties; decreased credit scores, lost work time, and other injuries. MoneyGram,

through its misconduct, has enabled numerous bad actors to sell and profit off of Prive Information that belongs to Plaintiff and the Class.

32. But for MoneyGram's unlawful conduct, scammers would not have access to Plaintiff's and the Class Members' contact information. MoneyGram's unlawful conduct has directly and proximately resulted in widespread digital attacks against Plaintiff and the Class.

Out of Pocket Costs

33. Plaintiff is now forced to research and subsequently acquire credit monitoring and reasonable identity theft defensive services and maintain these services to avoid further impact. Plaintiff anticipates spending out of pocket expenses to pay for these services.

34. MoneyGram also used Plaintiff's Private Information for profit and continued to use Plaintiff's Private Information to target Plaintiff, and share his information with various third parties, or to improve its marketing to other third parties for MoneyGram's own benefit.

Threat of Financial Fraud

35. The Data Breach has significantly increased the risk of financial fraud for affected customers. With access to sensitive financial information such as bank account numbers, transaction details, and MoneyGram's own loyalty program numbers, cybercriminals now have the tools to conduct unauthorized transactions or engage in financial identity theft.

36. Customers whose information was compromised in the Data Breach face an elevated risk of unauthorized money transfers or account takeovers and was the proximate consequence of MoneyGram's inability to secure its customers' Private Information.

Summary of Actual Economic and Noneconomic Damages

37. In sum, Plaintiff and similarly situated consumers were injured as follows:

i. Theft of their Private Information and the resulting loss of privacy rights in that information;

ii. Improper disclosure of their Private Information;

iii. Loss of value of their Private Information;

iv. The amount of ongoing reasonable identity defense and credit monitoring services made necessary as mitigation measures;

v. Defendant's retention of profits attributable to Plaintiff's and other customers' Private Information that Defendant failed to adequately protect;

vi. Economic and non-economic impacts that flow from imminent, and ongoing threat of fraud and identity theft to which Plaintiff is now exposed to;

vii. Ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of this data breach;

viii. Overpayments of Defendant's products and/or services which Plaintiff purchased;

ix. Emotional distress, and fear associated with the imminent threat of harm from the continued phishing scams and attacks as a result of this data breach.

CLASS ACTION ALLEGATIONS

38. Plaintiff brings this action on his own behalf and on behalf of all other persons similarly situated. The Class which Plaintiff seeks to represent comprises:

> All persons who used MoneyGram services in the United States and whose Private Information was accessed, compromised, or stolen in the data breach announced by MoneyGram on October 7, 2024.

This class definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

39. The California Subclass which Plaintiff seeks to represent comprises:

> All persons who used MoneyGram services in California and whose Private Information was accessed, compromised, or stolen in the data breach announced by MoneyGram on October 7, 2024." (the "**California Subclass**").

This class definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

40. The Class is comprised of millions of consumers throughout the United States and the state of California. The Class is so numerous that joinder of all members is impracticable and the disposition of their claims in a class action will benefit the parties and the Court.

41. There is a well-defined community of interest in the questions of law and fact involved and affecting the parties to be represented. The Class was exposed to the same common and uniform false and misleading representations and omissions. The questions of law and fact common to the Class predominate over questions which may affect individual Class members. Common questions of law and fact include, but are not limited to, the following:

a. Whether Defendant's conduct is an unlawful business act or practice within the meaning of Business and Professions Code section 17200, *et seq.*;

b. Whether Defendant's conduct is an unfair business act or practice within the meaning of Business and Professions Code section 17200, *et seq.*;

c. Whether Defendant's advertising as to its security practices is untrue or misleading within the meaning of Business and Professions Code section 17500, *et seq.*;

d. Whether Defendant's conduct is in violation of California Civil Code Sections 1709, 1710;

e. Whether Defendant's failure to implement effective security measures to protect Plaintiff's and the Class's Private Information negligent;

f. Whether Defendant breached express and implied warranties of security to the Class;

g. Whether Defendant represented to Plaintiff and the Class that they would protect Plaintiff's and the Class members' Private Information;

h. Whether Defendant owed a duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

i. Whether Defendant breached a duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

j. Whether Class members' PII was accessed, compromised, or stolen in the breach;

k. Whether Defendant's conduct caused or resulted in damages to Plaintiff and the Class;

l. Whether Defendant failed to notify the public of the breach in a timely and adequate manner;

m. Whether Defendant knew or should have known that its systems were vulnerable to a data breach;

n. Whether Defendant adequately addressed the vulnerabilities that allowed for the data breach; and

o. Whether, as a result of Defendant's conduct, Plaintiff and the Class are entitled to damages and relief.

42. Plaintiff's claims are typical of the claims of the proposed Class, as Plaintiff and the members of the Class were harmed by Defendant's uniform unlawful conduct.

43. Plaintiff will fairly and adequately represent and protect the interests of the proposed Class. Plaintiff has retained competent and experienced counsel in class action and other complex litigation.

44. Plaintiff and the Class have suffered injury in fact as a result of Defendant's false, deceptive, and misleading representations.

45. Plaintiff would not have sent money through the Platform but for the reasonable belief that Defendant would safeguard his data and Private Information.

46. The Class is identifiable and readily ascertainable. Notice can be provided to such purchasers using techniques and a form of notice similar to those customarily used in class actions, and by internet publication, radio, newspapers, and magazines.

47. A class action is superior to other available methods for fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it

impracticable or impossible for proposed members of the Class to prosecute their claims individually.

48. The litigation and resolution of the Class's claims are manageable. Individual litigation of the legal and factual issues raised by Defendant's conduct would increase delay and expense to all parties and the court system. The class action device presents far fewer management difficulties and provides the benefits of a single, uniform adjudication, economies of scale, and comprehensive supervision by a single court.

49. Defendant has acted on grounds generally applicable to the entire Class, thereby making final injunctive relief and/or corresponding declaratory relief appropriate with respect to the Class as a whole. The prosecution of separate actions by individual Class members would create the risk of inconsistent or varying adjudications with respect to individual member of the Class that would establish incompatible standards of conduct for Defendant.

50. Absent a class action, Defendant will likely retain the benefits of its wrongdoing. Because of the small size of the individual Class members' claims, few, if any, Class members could afford to seek legal redress for the wrongs complained of herein. Absent a representative action, the Class members will continue to suffer losses and Defendant (and similarly situated companies) will be allowed to continue these violations of law and to retain the proceeds of its ill-gotten gains.

COUNT ONE

VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW BUSINESS & PROFESSIONS CODE SECTION 17200, *et seq.* (ON BEHALF OF THE CALIFORNIA SUBCLASS AND NATIONWIDE CLASS)

51. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

52. For all Class members outside of the California Subclass, these claims are brought under the relevant consumer protection statute for the state in which they reside. For each state, the relevant statutes are as follows: Alabama—Deceptive Trade Practices Act (Ala. Code § 8-19-1, *et seq.*); Alaska—Unfair Trade Practices and Consumer Protection Act (Alaska Stat. §

45.50.471, *et seq.*); Arizona—Consumer Fraud Act (Ariz. Rev. Stat. Ann. § 44-1521, *et seq.*); Arkansas—Deceptive Trade Practices Act (Ark. Code Ann. § 4-88-101, *et seq.*); Colorado—Consumer Protection Act (Colo. Rev. Stat. § 6-1-101, *et seq.*); Connecticut—Connecticut Unfair Trade Practices Act (Conn. Gen. Stat. § 42-110a, *et seq.*); Delaware—Consumer Fraud Act (Del. Code Ann. tit. 6, § 2511, *et seq.*); District of Columbia—D.C. Code § 28-3901, *et seq.*; Florida—Deceptive and Unfair Trade Practices Act (Fla. Stat. § 501.20, *et seq.*); Georgia—Fair Business Practices Act (Ga. Code Ann. § 10-1-390, *et seq.*); Hawaii—Haw. Rev. Stat. § 480-1, *et seq.*); Idaho—Consumer Protection Act (Idaho Code Ann. § 48-601, *et seq.*); Illinois—Consumer Fraud and Deceptive Business Practices Act (815 Ill. Comp. Stat. 505/1, *et seq.*); Indiana—Deceptive Consumer Sales Act (Ind. Code § 24-5-0.5-1, *et seq.*); Iowa—Iowa Code § 7.14.16, *et seq.*); Kansas—Consumer Protection Act (Kan. Stat. Ann. § 50-623, *et seq.*); Kentucky—Consumer Protection Act (Ky. Rev. Stat. Ann. § 367.110, *et seq.*); Louisiana—Unfair Trade Practices and Consumer Protection Law (La. Rev. Stat. Ann. § 51:1401, *et seq.*); Maine—Unfair Trade Practices Act (Me. Rev. Stat. Ann. tit. 5, § 205A, *et seq.*); Maryland—Maryland Consumer Protection Act (Md. Code Ann., Com. Law § 13-101, *et seq.*); Massachusetts—Regulation of Business Practice and Consumer Protection Act (Mass. Gen. Laws Ann. ch. 93A, §§ 1-11); Minnesota—False Statement in Advertising Act (Minn. Stat. § 8.31, Minn. Stat. § 325F.67), Prevention of Consumer Fraud Act (Minn. Stat. § 325F.68, *et seq.*); Mississippi—Consumer Protection Act (Miss. Code Ann. § 75-24, *et seq.*); Missouri—Merchandising Practices Act (Mo. Rev. Stat. § 407.010, *et seq.*); Montana—Unfair Trade Practices and Consumer Protection Act (Mont. Code. Ann. § 30-14-101, *et seq.*); Nebraska—Consumer Protection Act (Neb. Rev. Stat. § 59-1601); Nevada—Trade Regulation and Practices Act (Nev. Rev. Stat. § 598.0903, *et seq.*, Nev Rev. Stat. § 41.600); New Hampshire—Consumer Protection Act (N.H. Rev. Stat. Ann. § 358-A:1, *et seq.*); New Jersey—N.J. Stat. Ann. § 56:8-1, *et seq.*); New Mexico—Unfair Practices Act (N.M. Stat. § 57-12-1, *et seq.*); New York—N.Y. Gen. Bus. Law §§ 349, 350, N.Y. Exec. Law § 63(12); North Carolina—N.C. Gen. Stat. § 75-1.1, *et seq.*); North Dakota—N.D. Cent. Code § 51-15-01, *et seq.*); Ohio—Consumer Sales Practices Act (Ohio Rev. Code Ann. § 1345.01, *et seq.*); Oklahoma—Consumer

Protection Act (Okla. Stat. tit. 15, § 751, *et seq.*); Oregon—Unlawful Trade Practices Law (Or. Rev. Stat. § 646.605, *et seq.*); Pennsylvania—Unfair Trade Practices and Consumer Protection Law (73 Pa. Stat. Ann. § 201-1, *et seq.*); Rhode Island—Unfair Trade Practice and Consumer Protection Act (R.I. Gen. Laws § 6-13.1-1, *et seq.*); South Carolina—Unfair Trade Practices Act (S.C. Code Ann. § 39-5-10, *et seq.*); South Dakota—Deceptive Trade Practices and Consumer Protection Law (S.D. Codified Laws § 37-24-1, *et seq.*); Tennessee—Consumer Protection Act (Tenn. Code Ann. § 47-18-101, *et seq.*); Texas—Deceptive Trade Practices—Consumer Protection Act (Tex. Bus. & Com. Code Ann. § 17.41, *et seq.*); Utah—Consumer Sales Practices Act (Utah Code Ann. § 13-11-1, *et seq.*); Vermont—Consumer Fraud Act (Vt. Stat. Ann. tit. 9, § 2451, *et seq.*); Virginia—Consumer Protection Act (Va. Code Ann. § 59.1-196, *et seq.*); Washington—Consumer Protection Act (Wash. Rev. Code § 19.86.010, *et seq.*); West Virginia—W. Va. Code § 46A-6-101, *et seq.*); Wisconsin—Wis. Stat. § 100.18, 100.20; Wyoming—Consumer Protection Act (Wyo. Stat. Ann. § 40-12-101, *et seq.*).

A. "Unfair" Prong

53. Under California's Unfair Competition Law, Cal. Bus. & Prof. Code Section 17200, *et seq.*, a challenged activity is "unfair" when "any injury it causes outweighs any benefits provide to consumers and the injury is one that the consumers themselves could not reasonably avoid." *Camacho v. Auto Club of Southern California*, 142 Cal. App. 4th 1394, 1403 (2006).

54. Defendant's conduct as alleged herein does not confer any benefit to consumers. It is especially questionable why Defendant would continue to store individual's data when it is unnecessary information for the handling of payments, such as when customers' identities have already been verified. Mishandling this data and a failure to archive and purge unnecessary data shows blatant disregard for customers' privacy and security.

55. Defendant did not need to collect the private data it did from its customers to allow use of the Platform. It did so to track and target its customers and monetize the use of the data to enhance its already exorbitant profits. Defendant utterly misused this data and Private Information.

56. Defendant's conduct as alleged herein causes injuries to consumers, who pay fees to send money on a Platform not consistent with their reasonable expectations of data security.

57. Defendant's conduct as alleged herein causes injuries to customers who entrusted Defendant with their Private Information and whose Private Information was leaked as a result of Defendant's unlawful conduct.

58. Defendant's failure to implement and maintain reasonable security measures was also contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. §45, California's Consumer Records Act, Cal. Civ. Code §1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

59. Consumers cannot avoid any of the injuries caused by Defendant's conduct as alleged herein.

60. The injuries caused by Defendant's conduct as alleged herein outweigh any benefits.

61. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes an unfair business practice within the meaning of California Business and Professions Code Section 17200.

62. Defendant could have furthered its legitimate business interests in ways other than by unfair conduct.

63. Defendant's conduct threatens consumers by misleadingly advertising their Platform as "secure" and exposing consumers' Private Information to hackers. Defendant's conduct also threatens other companies, large and small, who play by the rules. Defendant's conduct stifles competition and has a negative impact on the marketplace and reduces consumer choice.

64. All of the conduct alleged herein occurs and continues to occur in Defendant's business. Defendant's wrongful conduct is part of a pattern or generalized course of conduct repeated on approximately thousands of occasions daily.

65. Pursuant to Business and Professions Code Sections 17203, Plaintiff and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its unfair business practices.

66. Plaintiff and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiff relied on and chose to use, and pay fees on, the Platform in part based on Defendant's representations regarding its security measures and trusted that Defendant would keep his Private Information safe and secure. Plaintiff accordingly provided his Private Information to Defendant reasonably believing and expecting that his Private Information would be safe and secure. Plaintiff paid unwarranted fees to use the Platform. Specifically, Plaintiff paid fees to use a Platform advertised as secure when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiff and the Class would not have utilized the Platform, or would not have given Defendant their Private Information, had they known that their Private Information was vulnerable to a data breach. Likewise, Plaintiff and the members of the Class seek an order mandating that Defendant implement adequate security practices to protect consumers' Private Information. Additionally, Plaintiff and the members of the Class seek and request an order awarding Plaintiff and the Class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

B. "Fraudulent" Prong

67. California Business and Professions Code Section 17200, *et seq.* considers conduct fraudulent and prohibits said conduct if it is likely to deceive members of the public. *Bank of the West v. Superior Court*, 2 Cal. 4th 1254, 1267 (1992).

68. Defendant's representations that it adequately protects customers' Private Information is likely to deceive members of the public into believing that MoneyGram can be entrusted with their Private Information, and that Private Information gathered by MoneyGram is not in danger of being compromised.

69. Defendant's representations about its products and services, as alleged in the preceding paragraphs, are false, deceptive, misleading, and unreasonable and constitute fraudulent conduct.

70. Defendant knew or should have known of its fraudulent conduct.

71. As alleged in the preceding paragraphs, the material misrepresentations by Defendant detailed above constitute a fraudulent business practice in violation of California Business & Professions Code Section 17200.

72. Defendant could have implemented robust security measures to prevent the data breach but failed to do so.

73. Defendant's wrongful conduct is part of a pattern or generalized course of conduct.

74. Pursuant to Business & Professions Code Section 17203, Plaintiff and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its practice of false and deceptive representations about the strength or adequacy of its security systems. Likewise, Plaintiff and the Class seek an order requiring Defendant to disclose such misrepresentations.

75. Plaintiff and the Class have suffered injury in fact and have lost money as a result of Defendant's fraudulent conduct. Plaintiff paid unwarranted fees to use the Platform. Plaintiff would not have utilized the services, if he had known that the Platform's use would put his Private Information at risk.

76. **Injunction**. Pursuant to Business and Professions Code Sections 17203, Plaintiff and the Class seek an order of this Court compelling Defendant to implement adequate safeguards to protect all present and future customers' Private Information retained by Defendant, thereby seeking public injunctive relief that will benefit not only Plaintiff and the Class but also the members of the general public. This includes, but is not limited to: improving security systems, deleting data that no longer needs to be retained by Defendant, archiving that data on secure servers, and notifying all affected consumers in a timely manner.

C. "Unlawful" Prong

77. California Business and Professions Code Section 17200, *et seq.*, identifies violations of any state or federal law as "unlawful practices that the unfair competition law makes independently actionable." *Velazquez v. GMAC Mortg. Corp.*, 605 F. Supp. 2d 1049, 1068 (C.D. Cal. 2008).

78. Defendant's unlawful conduct, as alleged in the preceding paragraphs, violates California Civil Code Section 1750, *et seq.*

79. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes unlawful conduct.

80. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq*., the FTC Act, 15 U.S.C. § 45, and California common law. Defendant failed to notify all of its affected customers regarding said breach, failed to take reasonable security measures, or comply with the FTC Act, and California common law.

81. Defendant knew or should have known of its unlawful conduct.

82. As alleged in the preceding paragraphs, the misrepresentations by Defendant detailed above constitute an unlawful business practice within the meaning of California Business and Professions Code section 17200.

83. Defendant could have furthered its legitimate business interests in ways other than by its unlawful conduct.

84. All of the conduct alleged herein occurs and continues to occur in Defendant's business. Defendant's unlawful conduct is part of a pattern or generalized course of conduct repeated on approximately thousands of occasions daily.

85. Pursuant to Business and Professions Code Sections 17203, Plaintiff and the Class seeks an order of this Court enjoining Defendant from continuing to engage, use, or employ its unlawful business practices.

86. Plaintiff and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiff paid unwarranted fees to use the Platform. Specifically, Plaintiff paid to use a Platform advertised as secure when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiff and the Class would not have utilized the Platform, or would not have given Defendant their Private Information, had they known that their Private Information was vulnerable to a data breach. Likewise, Plaintiff and the members of the Class seek an order mandating that Defendant implement adequate security practices to protect customers' Private Information. Additionally, Plaintiff and the members of the Class seek and request an order awarding Plaintiff and the Class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

COUNT TWO
VIOLATION OF CALIFORNIA'S CONSUMER LEGAL REMEDIES ACT
CALIFORNIA CIVIL CODE SECTION 1750, *et seq.*
(ON BEHALF OF THE CALIFORNIA SUBCLASS)

87. Plaintiff repeats and re-alleges the allegations set forth in the preceding paragraphs and incorporates the same as if set forth herein at length.

88. The CLRA prohibits certain "unfair methods of competition and unfair or deceptive acts or practices" in connection with a sale of goods.

89. Defendant's unlawful conduct described herein was intended to increase the consuming public's use and fee payments for the use of its Platforms, and violated and continue to violate Section 1770(a)(5), (a)(7), and (a)(9) of the CLRA by representing that the Platform has characteristics and benefits which it does not have.

90. Defendant fraudulently deceived Plaintiff and the California Subclass by representing that its Platform has certain characteristics, benefits, and qualities which it does not

have, namely data protection and security. In doing so, Defendant intentionally misrepresented and concealed material facts from Plaintiff and the California Subclass, specifically by advertising secure technology when Defendant in fact failed to institute adequate security measures and neglected system vulnerabilities that led to a data breach. Said misrepresentations and concealment were done with the intention of deceiving Plaintiff and the California Subclass and depriving them of their legal rights and money.

91. Defendant's claims about its Platform led and continues to lead consumers like Plaintiff to reasonably believe that Defendant has implemented adequate data security measures when Defendant in fact neglected system vulnerabilities that led to a data breach and enabled hackers to access customers' Private Information.

92. Defendant knew or should have known that adequate security measures were not in place and that customers' Prviate Information was vulnerable to a data breach.

93. Plaintiff and the California Subclass have suffered injury in fact as a result of and in reliance upon Defendant's false representations.

94. Plaintiff and the California Subclass would not have utilized the Platform or would have accepted significantly reduced fees use of the Platform, had they known that their Private Information was vulnerable to a data breach, or that Defendant would fail to honor legal reporting requirements and leave them in the dark once their data was compromised.

95. Defendant's actions as described herein were done with conscious disregard of Plaintiff's rights, and Defendant was wanton and malicious in its concealment of the same.

96. Plaintiff and the California Subclass have suffered injury in fact and have lost money as a result of Defendant's unfair, unlawful, and fraudulent conduct. Specifically, Plaintiff and the Class paid unwarranted fees to use a Platform advertised as secure, and consequentially entrusted Defendant with their Private Information, when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiff and the California Subclass would not have utilized the Platform or would not have provided Defendant

with their Private Information, had they known that their Private Information was vulnerable to a data breach.

97. Defendant should be compelled to implement adequate security practices to protect its customers' Private Information. Additionally, Plaintiff and the members of the California Subclass lost money as a result of Defendant's unlawful practices.

98. At this time, Plaintiff seeks public injunctive relief under the CLRA pursuant to Cal. Civ. Code 1782(d); but he anticipates the need to amend the complaint and seek restitution.

COUNT THREE
VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")
CAL. CIV. CODE SECTION 1798.150, *et seq.*
(ON BEHALF OF THE CALIFORNIA SUBCLASS)

99. Plaintiff repeats and re-alleges the allegations set forth in the preceding paragraphs and incorporates the same as if set forth herein at length.

100. Defendant is a corporation organized or operated for the profit or financial benefit of its owners with annual gross revenues over $1.3 billion.[23]

101. Defendant collects consumers' personal information as defined in Cal. Civ. Code § 1798.140.

102. Defendant violated § 1798.150 of the CCPA by failing to prevent Plaintiff's and the California Subclass Members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

103. Defendant has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff's and California Subclass Members' PII. As detailed herein, Defendant failed to do so.

104. As a direct and proximate result of Defendant's acts, Plaintiff's and California Subclass Members' Private Information, including, names, contact information dates of birth,

[23] *Supra*, Note 1, at F-7 ("Consolidated Statements of Operations").

Social Security numbers, government-issued identification documents, bank account numbers, and transaction information, was subjected to unauthorized access and exfiltration, theft, or disclosure.

105. Plaintiff and California Subclass Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards customers' Private Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold customers' Private Information, including Plaintiff's and California Subclass Members' Prviate Information. Plaintiff and California Subclass Members have an interest in ensuring that their Prviate Information is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information, as evidenced by the Data Breaches.

106. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information to protect the Private Information under the CCPA.

107. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant and third parties with similar inadequate security measures.

108. Plaintiff and the California Subclass seek actual pecuniary damages, including actual financial losses resulting from the unlawful data breach.

COUNT FOUR
DECEIT BY CONCEALMENT, CALIFORNIA CIVIL CODE SECTIONS 1709, 1710
(ON BEHALF OF THE CALIFORNIA SUBCLASS)

109. Plaintiff herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

110. Defendant knew or should have known that its security systems were inadequate to protect the Private Information of its customers. Specifically, Defendant had an obligation to disclose to its customers that its security systems were not adequate to safeguard their Private

Information. Defendant did not do so. Rather, Defendant deceived Plaintiff and the California Subclass by concealing the vulnerabilities in its security system.

111. California Civil Code §1710 defines deceit as, (a) "[t]he suggestion, as a fact, of that which is not true, by one who does not believe it to be true"; (b) "[t]he assertion, as a fact, of that which is not true, by one who has no reasonable ground for believing it to be true"; (c) "[t]he suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact"; or (d) "[a] promise, made without any intention of performing it." Defendant's conduct as described herein therefore constitutes deceit of Plaintiff and the California Subclass.

112. California Civil Code §1709 mandates that in willfully deceiving Plaintiff and the California Subclass with intent to induce or alter their position to their injury or risk, Defendant is liable for any damage which Plaintiff and the California Subclass thereby suffer.

113. As described above, Plaintiff and the California Subclass have suffered significant harm as a direct and proximate result of Defendant's deceit and other unlawful conduct. Specifically, Plaintiff and the Class have been subject to numerous attacks, including various phishing scams. Defendant is liable for these damages.

COUNT FIVE
NEGLIGENCE
(ON BEHALF OF THE NATIONWIDE CLASS)

114. Plaintiff herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

115. Defendant owed a duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information. This duty included but was not limited to: (a) designing, implementing, and testing security systems to ensure that customers' Private Information was consistently and effectively protected; (b) implementing security systems that are compliant with state and federal mandates; (c) implementing security systems that are compliant with industry practices; and (d) promptly detecting and notifying affected parties of a data breach.

116. This duty arises because it is foreseeable that the exposure of Private Information to unauthorized persons, especially to perpetrators of cyberattacks with nefarious intentions, will result in harm to the affected individuals, including, but not limited to: the invasion of their private data, the sale of their Private Information to facilitate identity theft, exposure to scams or phishing frauds, loss of time, economic damages as affected individuals scramble to protect their identities, and/or the countless ways these individuals' peace of mind is destroyed knowing their information is no longer secured.

117. Defendant's duties to use reasonable care also arose from several sources, including those described below. As referenced above, Defendant had a common law duty to prevent foreseeable harm to others, including Plaintiff and members of the Class, who were the foreseeable and probable victims of any inadequate security practices.

118. Defendant's duties also arose under Section 5(a) of the Federal Trade Commission Act ("**FTC Act**") (15 USC § 45) prohibits "unfair or deceptive acts or practices in or affecting commerce." Defendant's failure to protect Plaintiff's and the Class members' Private Information constitutes an unfair or deceptive act or practice ("**UDAP**") because it (a) "causes or is likely to cause substantial injury to consumers;" (b) "cannot be reasonably avoided by consumers"; and (c) "is not outweighed by countervailing benefits to consumers or competition." As interpreted and enforced by the FTC, this includes the failure to use reasonable measures to protect customers' Private Information.

119. Defendant's duties arose in each state's data breach notification laws, which required Defendant to inform impacted customers when it learned their Private Information was accessed by a criminal. Those states relevant statutes are as follows: Alabama—Ala. Code § 8-38-10; Alaska—Alaska Stat. § 45.48.010 et seq; Arizona—Ariz. Rev. Stat. §§ 18-545; Arkansas—Ark. Code Ann. § 4-110-104; California—Cal. Civ. Code § 1798.82; Colorado—Colo. Rev. Stat. § 6-1-716; Connecticut—Conn. Gen. Stat § 36a-701b; Delaware—Del. Code Ann. tit. 6, § 12B-101 et seq.; District of Columbia—D.C. Code § 28- 3851 et seq.; Florida—Fla. Stat. § 501.171; Georgia—Ga. Code § 10-1-910, 10-1-912; Hawaii—Haw. Rev. Stat. § 487N-2; Idaho—Idaho

Stat. § 28-51-104 to 28-51-107; Illinois—815 ILCS 530/10; Indiana—Ind. Code § 24-4.9-3-1; Iowa—Iowa Code § 715C.2; Kansas—Kan. Stat. Ann. § 50-7a01 et seq.; Kentucky—Ky. Rev. Stat. Ann. § 365.732; Louisiana—La. Rev. Stat. § 51:3071 et seq.; Maine—Me. Rev. Stat. tit. 10, § 1347 et seq.; Maryland—Md. Code Ann., Com. Law § 14-3504; Massachusetts—Mass. Gen. Laws ch. 93H § 3; Michigan—Mich. Comp. Laws § 445.63; Minnesota—Minn. Stat. § 325E.61; Mississippi—Miss. Code Ann. § 75-24-29; Missouri—Mo. Rev. Stat. § 407.1500; Montana—Mont. Code Ann. § 30-14-1704; Nebraska—Neb. Rev. Stat. §§ 87-802, 87-803; Nevada—Nev. Rev. Stat. § 603A.220; New Hampshire—N.H. Rev. Stat. Ann. § 359-C:20; New Jersey—N.J. Stat. § 56:8-163; New Mexico—N.M. Stat. Ann. § 57-12C-1 et seq.; New York—GBL § 899-aa and N.Y. State Tech. Law § 208; North Carolina—N.C. Gen. Stat § 75-65; North Dakota—N.D. Cent. Code § 51-30-01 et seq.; Ohio—Ohio Rev. Code § 1349.19; Oklahoma—Okla. Stat. § 74-3113.1; Oregon—Or. Rev. Stat. § 646A.604; Pennsylvania—73 Pa. Stat. § 2303; Rhode Island—R.I. Gen. Laws § 11-49.2-1 et seq.; South Carolina—S.C. Code Ann. § 39-1-90; South Dakota—S.D. Codified Laws § 22-40-1; Tennessee—Tenn. Code Ann. § 47-18-2107; Texas—Tex. Bus. & Com. Code § 521.053; Utah—Utah Code § 13-44-201; Vermont—Vt. Stat. Ann. tit. 9, § 2430 et seq.; Virginia—Va. Code Ann. § 18.2-186.6; Washington—Wash. Rev. Code § 19.255.010; West Virginia—W. Va. Code § 46A-2A-101 et seq.; Wisconsin—Wis. Stat. § 134.98; Wyoming—Wyo. Stat. § 40-12-501 et seq.

120. Defendant knew or should have known that Plaintiff's and the Class members' Private Information is information that is frequently sought after by hackers.

121. Defendant knew or should have known that Plaintiff and the Class members would suffer harm if their Private Information was leaked.

122. Defendant knew or should have known that its security systems were not adequate to protect Plaintiff's and the Class Members' Private Information from a data breach, especially in light of the nature and sensitivity of the Private Information it collects and purports to safeguard.

123. Defendant knew or should have known that adequate and prompt notice of the data breach was required such that Plaintiff and the Class could have taken more swift and effective

action to change or otherwise protect their Private Information. Defendant failed to provide timely notice upon discovery of the data breach. The general public was informed of the Data Breach on October 9, 2024. However, Defendant has yet to notify all of the Class Members about the data breach, and thus, is continuing to impose harm on all individuals by failing to disclose who is affected by the data breach. Defendant had learned of the data breach on September 27, 2024.

124. Defendant's conduct as described above constituted an unlawful breach of its duty to exercise due care in collecting, storing, and safeguarding Plaintiff's and the Class members' Private Information by failing to design, implement, and maintain adequate security measures to protect this information.

125. Defendant and the Class entered into a special relationship when the Class members entrusted Defendant to protect their Private Information. Plaintiff and the Class paid fees to utilize Defendant's Platform, and in doing so provided Defendant with their Private Information, based upon Defendant's representations that it would implement adequate systems to secure their information. Defendant did not do so. Defendant knew or should have known that its security system was vulnerable to a data breach. Defendant breached its duty in this relationship to implement and maintain reasonable measures to protect the Private Information of the Class.

126. Plaintiff's and the Class members' Private Information would have remained private and secure had it not been for Defendant's wrongful and negligent breach of their duties. The leak of Plaintiff's and the Class members' Private Information, and all subsequent damages, was a direct and proximate result of Defendant's negligence.

127. Defendant's negligence was, at least, a substantial factor in causing the Plaintiff's and the Class's Private Information to be improperly accessed, disclosed, and otherwise compromised, and in causing the Class Members' other injuries because of the data breaches.

128. The damages suffered by Plaintiff and the Class members was the direct and reasonably foreseeable result of Defendant's negligent breach of its duties to adequately design, implement, and maintain security systems to protect Plaintiff and the Class Members' Private

Information. Defendant knew or should have known that its security for safeguarding Plaintiff and the Class Members' Private Information was vulnerable to a data breach.

129. Defendant's negligence directly caused significant harm to Plaintiff and the Class.

COUNT SIX
INTENTIONAL MISREPRESENTATION
(ON BEHALF OF THE NATIONWIDE CLASS)

130. Plaintiff repeats and realleges all of the allegations contained above and incorporate the same as if set forth herein at length.

131. Defendant has represented, through online advertisements and its privacy policy, that Defendant affords robust protection to its customers' Private Information.

132. Defendant makes representations that its security protections are multifaceted and effective, including the operation of "robust physical, technical, organizational, and administrative safeguards to protect [customers'] personal data from unauthorized access, loss or alteration."[24] and employing "preventive measures to restrict access to Personal Information to only those who have need to know"[25] Defendant in fact misrepresented the security of its services and products, failed to institute adequate security measures, and neglected vulnerabilities that led to a data breach of sensitive, personal information.

133. Defendant's misrepresentations regarding its security systems are material to a reasonable consumer, as they relate to the privacy of consumers' Private Information. A reasonable consumer would assign importance to such representations and would be induced to act thereon in making their purchase decision.

134. At all relevant times when such misrepresentations were made, Defendant knew or should have known that the representations were misleading.

135. Defendant intended for Plaintiff and the Class to rely on the representations of its security systems, as evidenced by Defendant's intentional marketing of a safe and secure Platform.

[24] *Supra,* Note 4.
[25] *Supra,* Note 8.

136. Plaintiff and members of the Class reasonably and justifiably relied on Defendant's intentional misrepresentations when paying fees to utilize the Platform, and had they known the truth, they would not have utilized the Platform or would not have given Defendant their Private Information.

137. Defendant was negligent in its representations that it would provide the highest level of security for consumers.

138. As a direct and proximate result of Defendant's intentional misrepresentations, Plaintiff and members of the Class have suffered injury in fact.

COUNT SEVEN

BREACH OF EXPRESS WARRANTY
(ON BEHALF OF THE NATIONWIDE CLASS)

139. Plaintiff repeats and realleges the allegations set forth above and incorporate the same as if set forth herein at length.

140. Defendant made an express warranty to Plaintiff and members of the Class that its security protections are multifaceted and effective. In order to utilize the Platform, Plaintiff and the Class were required to provide their Private Information which they reasonably believed, based on Defendant's expressed claims, would be kept private and secure.

141. Defendant's express warranty regarding its security standards it made to Plaintiff and the Class appears throughout its website and disclosures.[26] The promises of security associated with the products and services describes the products and services, specifically relates to the products/services being utilized and paid for, and therefore becomes the basis of the bargain.

142. Plaintiff and the Class paid fees for use of the Platform with the expectation that the information they provided would be kept safe, secure, and private in accordance with the express warranties made by Defendant on its website.

143. Defendant breached the express warranty made to Plaintiff and Class members by failing to provide adequate security to safeguard Plaintiff's and the Class's Private Information.

[26] *See supra* Notes 1-8.

As a result, Plaintiff and Class Members suffered injury and deserve to be compensated for the damages they suffered.

144. Plaintiff and Class Members paid fees for use of the Platform. However, Plaintiff and Class members did not obtain the full value of the advertised services. If Plaintiff and other Class members had known that their Private Information would be exposed, then they would not have utilized the Platform, or would have paid substantially less in fees to utilize the Platform.

145. Plaintiff and the Class are therefore entitled to recover all available remedies for said breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, prays for judgment and relief on all cause of action as follows:

A. That the Court determines that this Action may be maintained as a Class Action, that Plaintiff be named as Class Representative of the Class, that the undersigned be named as Lead Class Counsel of the Class, and that notice of this Action be given to Class Members;

B. That the Court enter an order declaring that Defendant's actions, as set forth in this Complaint, violate the laws set forth above;

C. An order:

   a. Prohibiting Defendant from engaging in the wrongful acts stated herein (including Defendant's failure to provide timely notice to all affected consumers);

   b. Requiring Defendant to implement adequate security protocols and practices to protect consumers' Private Information consistent with industry standards, applicable regulations, and federal, state, and/or local laws;

   c. Mandating the proper notice be sent to all affected consumers, and posted publicly;

d. Requiring Defendant to protect all data collected through its account creation or verification requirements;

e. Requiring Defendant to delete, destroy, and purge the Private Information of Plaintiff and Class Members unless Defendant can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

f. Requiring Defendant to implement and maintain a comprehensive security program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' Private Information;

g. Requiring Defendant to engage independent third-party security auditors and conduct internal security audit and testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

h. Requiring Defendant to engage independent third-party security auditors and/or internal personnel to run automated security monitoring;

i. Requiring Defendant to create the appropriate firewalls, and implement the necessary measures to prevent further disclosure and leak of any additional information;

j. Requiring Defendant to conduct systematic scanning for data breach related issues;

k. Requiring Defendant to train and test its employees regarding social engineering protocols and appropriate responses to such attempts, including any necessary ongoing training, on a periodic basis, to ensure that its employees are well-versed in recognizing and capable of preventing, a social engineering attempt to access its data systems;

l. Requiring Defendant to train and test its employees regarding data breach protocols, archiving protocols, and conduct any necessary employee background checks to ensure that only individuals with the appropriate training and access may be allowed to access the PII data; and

m. Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

D. That the Court award Plaintiff and the Class damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;

E. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution, and/or disgorgement) against Defendant to which Plaintiff and the Class are entitled, including but not limited to restitution and an Order requiring Defendant to cooperate and financially support civil and/or criminal asset recovery efforts;

F. That the Court award Plaintiff and the Class pre- and post-judgment interest (including pursuant to statutory rates of interest set under State law);

G. That the Court award Plaintiff and the Class their reasonable attorneys' fees and costs of suit;

H. That the Court award treble and/or punitive damages insofar as they are allowed by applicable laws; and

I. That the Court award any and all other such relief as the Court may deem just and proper under the circumstances.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff respectfully demands a trial by jury for all claims.

Dated: October 10, 2024

Respectfully submitted,

/s/ Darren Nicholson

Warren T. Burns
Texas Bar No. 24053119
Darren Nicholson
Texas Bar No. 24032789
Chase Hilton
Texas Bar No. 24100866
BURNS CHAREST LLP
900 Jackson Street, Suite 500
Dallas, Texas 75202
Tel: (469) 904-4550
wburns@burnscharest.com
dnicholson@burnscharest.com
chilton@burnscharest.com

Ryan J. Clarkson *(pro hac vice to be submitted)*
Yana Hart *(pro hac vice to be submitted)*
Tiara Avaness *(pro hac vice to be submitted)*
CLARKSON LAW FIRM, P.C.
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
rclarkson@clarksonlawfirm.com
yhart@clarksonlawfirm.com
tavaness@clarksonlawfirm.com

Counsel for Plaintiff and the Putative Classes